What is claimed is:

Sub B9

1. In a system having one or more security mechanisms, a method of defining and enforcing a security policy, the method comprising:

encapsulating security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key for each security mechanism;

combining keys to form key chains;

encapsulating key chains as keys and passing the key chain keys to another semantic layer;

defining the security policy, wherein defining includes forming key chains from keys and associating users with key chains;

translating the security policy and exporting the translated security policy to the security mechanisms; and

enforcing the security policy via the security mechanisms.

2. The method of claim 1 wherein the security mechanisms are located on one or more distributed computer networks.

3. The method of claim 1 wherein the security mechanisms are heterogeneous.

4. The method of claim 1, wherein defining the security policy further includes drilling down into a next lower semantic layer to form a new key chain.

5. The method of claim 1 wherein the security policy is defined using a graphical user interface.

6. A security system comprising:

a plurality of security mechanisms;

a plurality of semantic layers, including a first semantic layer, wherein the first semantic layer combines keys, wherein each key encapsulates security mechanism application specific information for a security mechanism;

a user interface for defining a security policy as a function of keys received from a lower semantic layer; and

a translator for translating the security policy to the security mechanisms.

7. The system according to claim 6 wherein the user interface is a graphical user interface.

8. The system according to claim 6 wherein the security policy is a role-based access control model.

9. The system of claim 6 wherein the semantic layers form a poset.

10. The system of claim 6 wherein the user interface includes means for drilling down into a lower semantic layer to form a new key chain.

11. A security system comprising:

a model comprising one or more semantic layers for defining different security policies and constraints for each type of user;

a tool for manipulating the model; and

a translator for translating security policies from the model to security mechanisms in one or more computer resources.

12. The method of claim 11 wherein the model comprises a static application policy layer, one or more semantic policy layers, and a dynamic local policy layer.

13. The method of claim 11 wherein the model represents a set of access rights for a computer resource as a key and the model represents a set of keys as a key chain.

14. A method of defining a security policy, the method comprising:

defining an application policy layer and a plurality of semantic policy layers, including a first semantic policy layer and a second semantic layer;

encapsulating a set of access rights for a computer resource as a key;

combining keys to form one or more key chains within the application policy layer;

exporting key chains in the application policy layer as a key;

importing at least one key from the application policy layer into the first semantic policy layer;

combining one or more keys in the first semantic policy layer to form a key chain;

exporting key chains in the first semantic policy layer as keys;

importing at least one key into the second semantic policy layer;

combining one or more keys in the second semantic policy layer to form a key chain;

exporting key chains in the second semantic policy layer as keys;

importing at least one key from the second semantic policy layer to a local policy layer;

combining one or more keys in the local policy layer to form one or more local policy key chains; and

assigning users to local policy key chains in the local policy layer.

15. The method of claim 14 wherein combining one or more keys to form a key chain includes combining a key chain with the one or more keys to form another key chain.

16. The method of claim 14 wherein combining one or more keys in the first semantic layer includes combining a key chain with the one or more keys to form another key chain.

17. The method of claim 14 wherein combining one or more keys to form a key chain includes associating a constraint with the key chain, wherein the constraint must be satisfied before access to a computer resource governed by the key chain is granted.

18. The method of claim 14 wherein encapsulating includes grouping methods into handles and handles into keys.

19. The method of claim 18 wherein each key chain includes handles for different computer resources.

20. The method of claim 14 wherein combining one or more keys to form a key chain includes marking the key chain as abstract, wherein key chains marked as abstract are not exported to other layers.

21. The method of claim 14 further comprising combining one or more keys and key chains in the local policy layer to form a new key chain in the local policy layer.

22. A method of defining a security policy, the method comprising:

defining an application policy layer and a semantic policy layer;

encapsulating a set of access rights for a computer resource as a key;

combining keys to form one or more key chains within the application policy layer;

exporting key chains in the application policy layer as a key;

importing at least one key from the application policy layer into the semantic policy layer;

combining one or more keys in the semantic policy layer to form a key chain;

exporting key chains in the semantic policy layer as keys;

importing at least one key from the semantic policy layer to a local policy layer;

combining one or more keys in the local policy layer to form one or more local policy key chains; and

assigning users to local policy key chains in the local policy layer.

23. The method of claim 22 wherein combining one or more keys in the semantic policy layer to form a key chain includes combining a key chain with the one or more keys to form another key chain.

24. The method of claim 22 wherein combining one or more keys in the local policy layer to form a key chain includes combining a key chain with the one or more keys to form another key chain.

25. The method of claim 22 wherein combining one or more keys in the semantic policy layer to form a key chain includes associating a constraint with the key chain, wherein the constraint must be satisfied before access to a computer resource governed by the key chain is granted.

26. The method of claim 22 wherein combining one or more keys in the local policy layer to form a key chain includes associating a constraint with the key chain, wherein the constraint must be satisfied before access to a computer resource governed by the key chain is granted.

27. The method of claim 22 wherein encapsulating includes grouping methods into handles and handles into keys.

28. The method of claim 27 wherein each key chain includes handles for different computer resources.

29. The method of claim 22 wherein combining one or more keys to form a key chain includes marking the key chain as abstract, wherein key chains marked as abstract are not exported to other layers.

30. The method of claim 22 further comprising combining one or more keys and key chains in the local policy layer to form a new key chain in the local policy layer.

31. A method of modifying a security policy, the method comprising:

defining an application policy layer and a semantic policy layer;

encapsulating a set of access rights for a computer resource as a key;

combining keys to form one or more key chains within the application policy layer;

exporting key chains in the application policy layer as a key;

importing at least one key from the application policy layer into the semantic policy layer;

combining one or more keys in the semantic policy layer to form a key chain;

exporting key chains in the semantic policy layer as keys;

importing at least one key from the semantic policy layer to a local policy layer;

combining one or more keys in the local policy layer to form one or more local policy key chains;

assigning users to local policy key chains in the local policy layer;

constructing a role hierarchy by sorting the key chains into a partial ordering based on set containment;

displaying the partial ordering as a role hierarchy graph; and

adding and deleting keys from the role hierarchy graph.

32. An article comprising a computer readable medium having instructions thereon, wherein the instructions, when executed in a computer, create a system for executing the method of claim 1.

33. An article comprising a computer readable medium having instructions thereon, wherein the instructions, when executed in a computer, create a system for executing the method of claim 14.

34. An article comprising a computer readable medium having instructions thereon, wherein the instructions, when executed in a computer, create a system for executing the method of claim 22.

35. An article comprising a computer readable medium having instructions thereon, wherein the instructions, when executed in a computer, create a system for executing the method of claim 31.

36. In a system having a workflow management system and a central policy management system, a method of controlling workflow, comprising:

creating a workflow class definition;

exporting the workflow class definition to the central policy management system;

binding resources and roles to steps within the central policy management system;

creating a workflow instance in both the workflow management system and the central policy management system; and

executing the workflow instance.

37. An article comprising a computer readable medium having instructions thereon, wherein the instructions, when executed in a computer, create a system for executing the method of claim 36.

38. A workflow control system, comprising:

a workflow management system; and

a central policy management system;

wherein the workflow management system creates a workflow class definition and exports the workflow class definition to the central policy management system; and

wherein resources and roles are bound to steps within the central policy management system.